РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

ПРЕЗЕНТАЦИЯ ПО ЛАБОРАТОРНОЙ РАБОТЕ №6

дисциплина: Математические основы защиты информации и информационной безопасности

Преподователь: Кулябов Дмитрий Сергеевич

Студент: Попова Юлия Дмитриевна

Группа: НФИмд-01-23

МОСКВА

2023 г.

Прагматика выполнения лабораторной работы

Требуется реализовать:

1. Алгоритм, реализующий p-метод Полларда

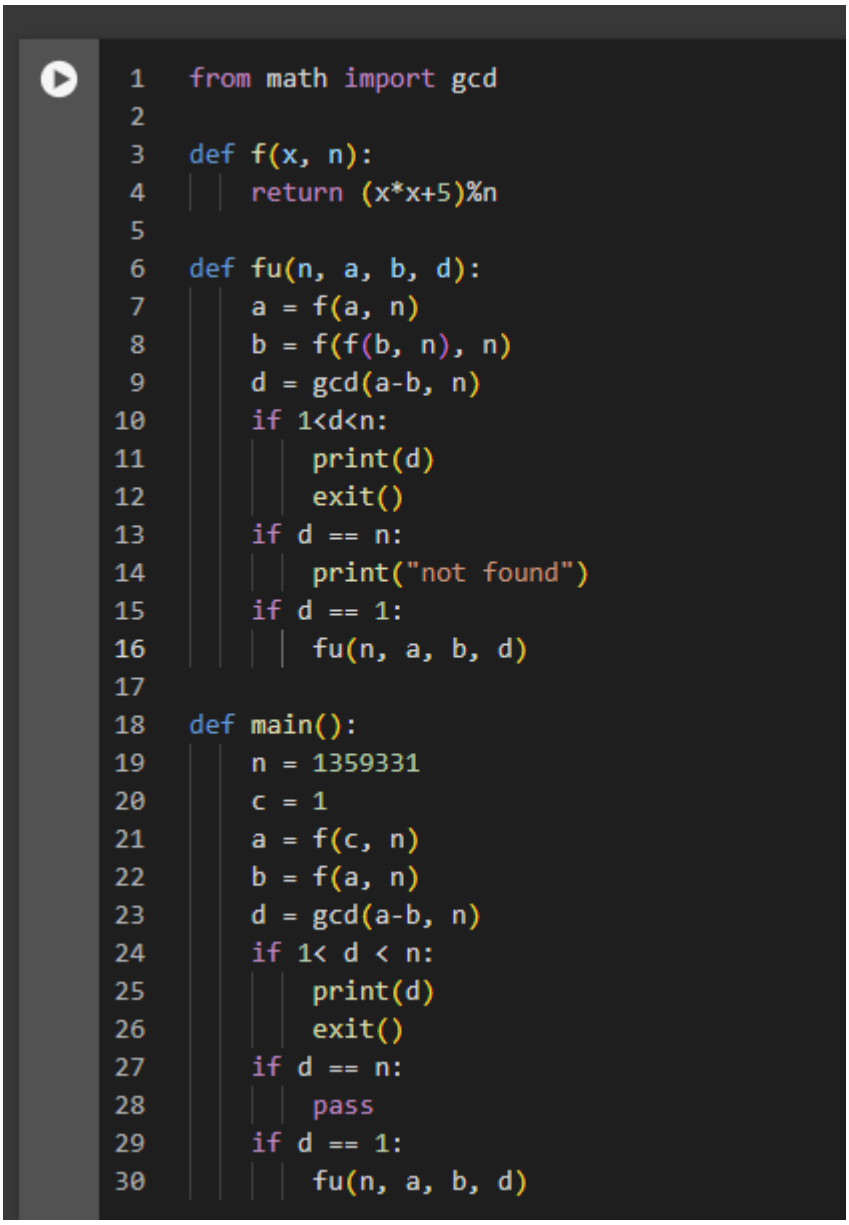
Цель работы

Освоить на практике разложение чисел на множители.

Выполнение лабораторной работы

1. Для реализации p-метода Полларда:

1. Функция, реализующая p-метод Полларда
2. Функция нахождения НОД



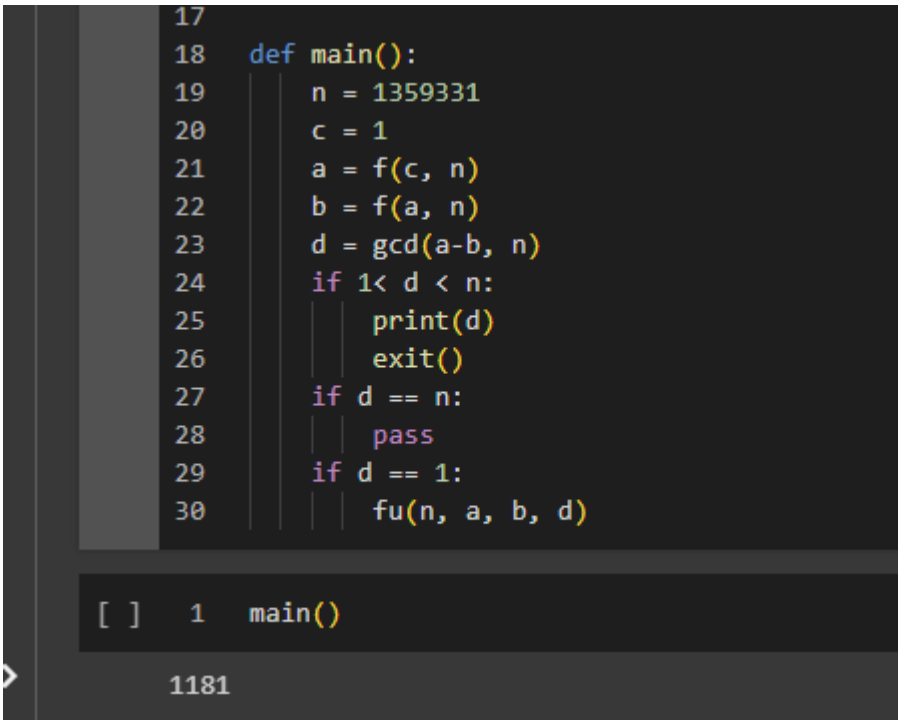
```python
from math import gcd

def f(x, n):
    return (x*x+5)%n

def fu(n, a, b, d):
    a = f(a, n)
    b = f(f(b, n), n)
    d = gcd(a-b, n)
    if 1<d<n:
        print(d)
        exit()
    if d == n:
        print("not found")
    if d == 1:
        fu(n, a, b, d)

def main():
    n = 1359331
    c = 1
    a = f(c, n)
    b = f(a, n)
    d = gcd(a-b, n)
    if 1< d < n:
        print(d)
        exit()
    if d == n:
        pass
    if d == 1:
        fu(n, a, b, d)
```

2. Основная фунция запуска где получаем входные значения и шифруем слово



```
17
18  def main():
19      n = 1359331
20      c = 1
21      a = f(c, n)
22      b = f(a, n)
23      d = gcd(a-b, n)
24      if 1< d < n:
25          print(d)
26          exit()
27      if d == n:
28          pass
29      if d == 1:
30          fu(n, a, b, d)
```

```
[ ]  1  main()
```

```
1181
```

Выводы

В результате выполнения работы освоили на практике алгоритм разложения чисел на множители.